Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1978

Vragen van het lid **De Caluwé** (VVD) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *de proef met het publieke middel voor online inloggen bij de overheid* (ingezonden 17 februari 2016).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 23 maart 2016)

Vraag 1
Heeft u kennisgenomen van het artikel van RTL «Deze elektronische identiteitskaart vervangt straks DigiD»?[1]

Antwoord 1
Ja.

Vraag 2
Wat is uw reactie op de volgende opgevoerde quote van de woordvoerster van het ministerie: «Wanneer iedereen met zijn ID-kaart kan inloggen, is nog niet duidelijk, de invoering zal nog wel enkele jaren op zich laten wachten»?

Antwoord 2
De elektronische Nederlandse Identiteitskaart (verder: eNIK) is naar verwachting eind 2017 voor iedereen beschikbaar. Het is echter aan de burger zelf om te beslissen wanneer een geldige NIK omgewisseld wordt voor een eNIK.
De NIK is 10 jaar geldig. Tot nu toe is uitgegaan van een natuurlijk vervangingspatroon, dit in verband met kosten en uitvoeringsvraagstukken. In dat geval moet rekening gehouden worden met een maximale omwisselingtermijn van 10 jaar. Ik laat onderzoeken of en zo ja hoe deze omwisselingstermijn kan worden verkort.
Overigens wordt thans ook ingezet op de versterking van het huidige publieke middel DigiD door middel van een extra controle na het inloggen door het uitlezen van gegevens op de chip van een wettelijk identiteitsdocument, zoals de Nederlandse identiteitskaart en het rijbewijs. Deze optie is op dit moment onderwerp van een pilot.
Voor de *algehele* invoering van de eNIK is de woordvoerster van het ministerie derhalve uitgegaan van een langere periode dan enkele jaren.

[1] http://www.rtlnieuws.nl/economie/home/deze-elektronische-identiteitskaart-vervangt-straks-digid

ah-tk-20152016-1978
ISSN 0921 - 7398
’s-Gravenhage 2016

Vraag 3
Hoe verhoudt de hierboven genoemde uitspraak zich tot de motie-De Caluwé (Kamerstuk 26 643 nr. 376) dat er in 2017 in ieder geval één publiek middel moet zijn?

Antwoord 3
Ik houd vast aan eerdere berichtgeving[2] en de door u ingediende motie dat een publiek middel in 2017 beschikbaar moet zijn.

Vraag 4
Wat is uw reactie op de vermelding in het artikel dat de proeven dit hele jaar lopen, terwijl u steeds heeft aangegeven dat de proeven medio dit jaar afgerond en geëvalueerd worden?

Antwoord 4
Conform afspraak met uw Kamer zijn er proeven opgezet. Aan de hand van deze proeven en de evaluatie brengt, op verzoek van uw Kamer, de ingestelde commissie Kuipers een advies uit aan mijn collega van Economische Zaken en mijzelf, waarna het kabinet medio 2016 een standpunt over de uitrol van onder andere het publieke authenticatiemiddel en de inzet van private authenticatiemiddelen zal voorbereiden.[3]
De meeste proeven lopen tot medio 2016. Enkele proeven in het BSN-domein, waaronder die in de zorg, starten later (april 2016) en hebben daarom ook een einddatum na medio 2016.
Voorop staat dat in alle gevallen het een kleinschalige beproeving van nieuwe middelen betreft, waarbij het niet gaat om een feitelijk grootschalige uitrol. Er wordt vastgehouden aan de afspraak met de Kamer dat een multimiddelen-strategie beproefd wordt.
Overigens is het praktisch onmogelijk om de proeven in het BSN-domein grootschalig te verlengen na medio 2016. Immers het BSN-koppelregister, welke noodzakelijk is voor de toegang van een privaat middel tot het BSN-domein, is ingericht voor de pilotfase met een beperkte verwerkingscapaciteit. Voor een definitieve uitrol moet het BSN-koppelregister aangepast worden om meer te kunnen verwerken.
Ik wijs er voor de volledigheid op dat, zoals de Kamer gemeld is, dit jaar ook proeven worden gedaan tussen bedrijven en hun klanten op basis van het onder verantwoordelijkheid van mijn collega van Economische Zaken gemaakte Idensys afsprakenstelsel. Omdat deze proeven zich afspelen in het private domein is de doorlooptijd van deze proeven en/of de definitieve uitrol van de middelen aan deze partijen zelf.

Vraag 5
Wat is uw reactie op uitlatingen van professor Hoepman in genoemd artikel, dat wij straks zelf geen sleutel in handen hebben, maar uitsluitend de tussenpersoon, oftewel «de conciërge»?

Antwoord 5
De metafoor van de authenticatiedienst als conciërge versimpelt de complexiteit van digitale toegangsdiensten, maar laat daardoor ook veel zaken buiten beschouwing. De authenticatiedienst is gebonden aan strikte voorschriften, waaronder eisen inzake de bescherming van persoonsgegevens en Europese eisen.[4]

---

[2] Tweede Kamerbrief van 14 december 2015, kst. 26 643 nr. 379.
[3] Tweede Kamerbrief van 17 november 2015, 26 643 nr. 371.
[4] VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. Klik hier voor de officiële tekst.
En:
UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt. Klik hier voor de officiële tekst.

Ik vind net als de heer Hoepman dat de gebruiker in controle moet zijn van zijn eigen digitale identiteit, transacties en persoonsgegevens. In de digitale wereld is het de taak van de authenticatiedienst om de gebruiker te ondersteunen in het veilige gebruik van zijn authenticatiemiddel. Daarbij moet de privacy van burgers natuurlijk goed beschermd worden. Voor mij staan deze eisen centraal bij een onafhankelijke beoordeling van de pilots en de verdere uitrol.

Vraag 6
Wat is uw reactie op uitlatingen van professor Hoepman, dat commerciële aanbieders straks weten waar wij allemaal inloggen, terwijl u steeds heeft aangegeven dat dit soort verzameling van gegevens (hotspots) niet gaat plaatsvinden?

Antwoord 6
Zoals in de Tweede Kamerbrief van 14 december 2015[5] is gesteld worden voor authenticatiediensten in het publieke domein strikte informatiebeveiligingsnormen gesteld, die verplichte versleuteling, eisen aan de opslag van persoonsgegevens en dataminimalisatie borgen. Ook worden er privacybeschermende maatregelen genomen. Bijvoorbeeld om het verzamelen van de gegevens over het inloggedrag van een gebruiker tegen te gaan.
Voor de pilotfase is een Privacy Impact Assessment (PIA) uitgevoerd, waarbij getoetst is aan feitelijke en technische nationale en Europese juridische privacyvereisten.[6] Uit de PIA is gebleken dat voor de pilotfase de privacymaatregelen adequaat zijn, maar dat voor een eventuele structurele fase bovengenoemde maatregelen in de rede liggen.

---

[5] Tweede Kamerbrief van 14 december 2015, kst. 26 643 nr. 379.

[6] Een PIA is een hulpmiddel bij de ontwikkeling van beleid, wetgeving en bouw van IT-systemen. Hiermee kunnen privacyrisico’s op een gestructureerde en heldere wijze in kaart worden gebracht.